Brussels, 2 September 2021
CDO

EACB Key Messages on the Commission's Data Act Public Consultation

The **European Association of Co-operative Banks** (EACB) represents, promotes and defends the common interests of its 27 member institutions and of cooperative banks, with regard to banking as well as to co-operative legislation. Founded in 1970, today the EACB is a leading professional lobbying association in the European banking industry. Co-operative banks play a major role in the financial and economic system. They contribute widely to stability thanks to their anti-cyclical behaviour, they are driver of local and social growth with 2.800 locally operating banks and 51,500 outlets, they serve 209 million customers, mainly consumers, SMEs and communities. Europe's co-operative banks represent 84 million members and 713,000 employees and have an average market share in Europe of about 20%.

For further details, please visit www.eacb.coop

EACB AISBL – Secretariat • Rue de l'Industrie 26-38 • B-1040 Brussels
Tel: (+32 2) 230 11 24 • Fax (+32 2) 230 06 49 • Enterprise 0896.081.149 • lobbying register 4172526951-19
www.eacb.coop • e-mail : secretariat@eacb.coop

Introduction

The European Association of Co-operative Banks (EACB) is happy to contribute to the discussion on the Data Act.

We support the Commission's general principle of facilitating the sharing of data based on free decision about voluntary data sharing or data sharing on a contractual basis.

Before going into the specific answers of the Commission's public consultation, we would like to note that providing comprehensive answers to the consultation document was challenging due to the way the consultation was built (e.g., to respond yes/no or fill in tables with multiple entries). For this reason, we decided not to answer some of the questions but provide you with our responses to many of the questions in the various sections here below.

EACB's comments

SECTION I. Business-to-government data sharing for the public interest

Have you or has your organisation experienced difficulties/encountered issues when requesting or responding to requests for access to data, in the context of B2G data sharing for the public interest?

Based on the feedback received from EACB members, i.e., the national co-operative associations and /or co-operative banks across Europe, we are not aware of any major issues related to B2G for the public interest. In our experience B2G data sharing happens mostly in the context of sharing that is necessary to fulfil legal/regulatory obligations which are clearly defined by law.

Should the EU take additional action so that public sector bodies can access and re-use private sector data, when this data is needed for them to carry out their tasks in the public interest purpose?

Access to and re-use of private-sector data in the public interest are important topics which may require legislative action. However, access and re-use will need to be linked to the specific public interests pursued by the relevant public-sector bodies, which will be different for different sectors and use cases. As such, sectorial legislation might be more appropriate to specify the necessary goals and conditions.

In this context, it must be considered that there are already laws at national level which define and regulate public sector bodies' access to and re-use of private sector data when such data is needed to carry out their tasks in the public interest. In general, public interest is the subject of extensive legislation at national level.

In which of the following areas do you think that, for specific use-cases with a clear public interest, B2G data sharing should be compulsory, with appropriate safeguards?

As said in our previous answer, any mandatory access needs to be strictly linked to the specific public interests pursued. As such, given the invasiveness of mandatory access, extensive impact analyses must be conducted to verify and justify the goals pursued and conditions identified for each individual use case where mandated access is being explored. As a rule, beyond existing legislative or regulatory areas, access and re-use should be pursued on a voluntary as opposed to mandatory fashion in order to generate a positive innovation dynamic between the private and public sector based on mutual benefit and trust.

When sharing data with public bodies, businesses should provide it: (For free/at a preferential rate/ below market price (marginal cost or other)/At market price/Depending on the purpose it may be provided at market price, preferential rate or for free)

A one-size-fits-all solution to the question of price cannot be given. Given the invasiveness of mandatory access, price as well as all other aspects must be subject to an extensive impact analysis for each individual use case where mandated access is being explored.
As a rule, beyond existing legislative or regulatory areas, access and re-use should be pursued on a voluntary as opposed to mandatory fashion in order to generate a positive innovation dynamic between the private and public sector based on mutual benefit and trust. We are confident that the market will efficiently explore possibilities for access and re-use, and that regulatory intervention should be restrained so as not to stifle innovation. We would like to point out that the market is still learning its lessons from PSD2.

In general, as underlined in the High-Level Expert Group on Business-to-Government Data Sharing report, the level of compensation for acquiring data should, in principle, be linked to the effort and investment required by the private company or civil-society organisation for making it available. More specifically, it could be linked to the type of data shared: raw, (pre-) processed, data driven insights. We note that even sharing of raw data will imply costs (e.g., for managing the necessary infrastructure, regulatory reporting, etc.) which should be compensated.

The overall investment should at least partially be taken into account, not just the investment in precisely the data shared. Notably, research and development activities include many failures never giving a return on investment. The aim is not to upset these economic models which are essential for innovation in Europe. It is also important that the cost of formatting the data is taken into account in the price of sharing.

What safeguards for B2G data sharing would be appropriate?

We believe that all the safeguards mentioned in the consultation are important (i.e., data security measures including protection of commercially sensitive information; specific rules on proportionality and reasonableness of the request; transparent reporting on how the public authority has used the data; limitations regarding how long public bodies may use or store specific datasets before having to destroy them). However, the specific safeguards (for example conditions for pseudonymization or anonymization) to be used will also be contingent on the

specific objectives and use-cases to be pursued, subject to the necessary impact assessment as underlined in our responses to the previous questions.

Clear measures tailored to the specific uses are vital in order to remove legal uncertainty, particularly in terms of compliance with the GDPR.

Which of the following types of financial compensation would incentivise you to engage in a B2G data-sharing collaboration for the public interest (select all that apply)?

Marginal costs for dissemination plus fair return on investment (ROI) or market price would be the preferred types of financial compensation that would incentivise EACB members to engage in a B2G data-sharing collaboration for the public interest.

Which of the following types of non-monetary compensation would incentivise you to engage in a B2G data-sharing collaboration for the public interest (select all that apply)?

Based on the feedback received from EACB members, tax incentives, increased know-how and innovation through co-creation with public bodies, reputation/ public recognition programmes (e.g., corporate social responsibility), investment of public funds to support the development of trusted technical tools for B2G data sharing would be the types of non-monetary compensation that would incentivise EACB members to engage in a B2G data-sharing collaboration for the public interest.

EACB members believe that an effective system of incentives, which could also be considered as a way to cover the costs associated with sharing, is crucial to boost the private-sector willingness to engage in public-private projects. As we highlighted in previous responses, sharing should as a rule be voluntary.

SECTION II. Business-to-business data sharing

Does your company share data with other companies? (This includes providing data to other companies and accessing data from other companies). How often in the last five years? Please describe the type of data shared, and the type of businesses with whom it is shared.

EACB members have been sharing data with other companies many times in the last five years as both data holder and user.

Sharing as reported by our members happens primarily: within the same group; with other companies pursuant to the PSD2; or with other companies (e.g., banks or credit providers) and public authorities pursuant to legal obligations (for example in the payment fraud or payment default fields).

In terms of the type of data shared, EACB members shared personal and non-personal payment accounts of customers' data (due to PSD2, banks have implemented specific APIs for third party provider – Account Information Service Providers or Payment Initiation Service Providers.

When it is shared within the same group/network, generally, the data shared is primarily benchmark data for comparison including consumer behaviour, general business data, etc.

On what basis does your company share data with other companies? Why does your company share data with other companies?

EACB members share data with other companies on both voluntary and mandatory basis.

In addition to the options listed in the questionnaire (i.e., optimisation of the supply chain, training algorithms for AI, design of innovative solutions/products), EACB members share data with other companies to fulfil legal obligations such as PSD2, AML/CTF purposes, and based on legitimate interest, e.g., to manage operation in multiple Member States, using benchmark to improve internal processes and drive the use of digital solutions. Data is also shared in the context of ad-hoc initiatives such as Open Data platforms, academic collaborations, innovation programs with start-ups etc.

Which services/products based on data sharing exist/are under development in your sector and what type of data are needed for these purposes?

EACB members develop parts of their product portfolios based on data sharing and use of personal and non-personal customer data (e.g., KYC data, transaction data, pricing data).

The business use of data is not limited to product and service development. It also allows better targeting, better advice, better knowledge of customers, better risk management (e.g., development of predictive/preventive approach or data improvement, sectorial classification, internal/external data cross checking). Sharing in the context of digital client communication such as online banking, online services, mobile apps, etc. is also vital for the development and delivery of digital solutions.

What benefits from data sharing do you expect to be reaped in your sector?

EACB members see the following benefits from data sharing: scalability; better knowledge of customers for the development of new products and services adapted to their needs; more efficient predictive models; more resources to train AI models; a better understanding of the underlying risks or counterparty behaviour in order to improve risk management; predictive marketing; process automation; prevention and assistance (insurance).

Has your company experienced difficulties/encountered issues when requesting access to other companies' data? How often in the last 5 years?

EACB members have very often experienced difficulties/encountered issues when requesting access to other companies' data in the last five years.

EACB members indicated having experienced difficulties such as those mentioned in the consultation (i.e., the data holder refused to give data on the basis of competition law concerns; the data holder refused to give access to data for reasons other than competition law concerns; the data holder is prevented by law to give access to data; there is no legal basis for the data holder to give access to data; the data holder gave access to data at unreasonable conditions, e.g. unilateral change of contractual terms, disproportionate restriction of use of data, limitations in the termination of contract; the data holder gave access to data at an unreasonable price; technical reasons like the data was not in usable format or quality or lacks shared vocabularies or metadata or the data holder doesn’t support standards for enforce data usage controls

(connector)). Members stressed that they have encountered difficulties due to a lack of standards; possible syntax errors; terms of the data provider authorized only a limited set of uses and under specific conditions; data provided not including reliability indicators; a technical format imposing fixed data sets and not in real time.

We would also like to stress that some national laws prevent data access such as local bank secrecy regulations.

Do you agree that the application of a 'fairness test', to prevent unilateral imposition by one party of unfair contractual terms on another, could contribute to increasing data sharing between businesses (including for example co-generated non-personal IoT data in professional use)? Do you agree that model contract terms for voluntary use in B2B data sharing contracts could contribute to increasing data sharing between businesses (including for example co-generated non-personal IoT data in professional use)? Do you agree that horizontal access modalities based on variations of fair, reasonable and non-discriminatory conditions applicable to data access rights, established in specific sectors, could contribute to increasing data sharing between businesses (including for example co-generated non-personal IoT data in professional use)?

These topics raise many questions. A 'fairness test' implies fundamental questions about who would perform such test, what criteria would be used, etc. A generalised use of FRAND in legislation fundamentally misunderstands the link of this concept with the fields in which it is presently used (notably its special use in standardisation), which cannot be generalised.

As much as we welcome the idea to base data exchange on fairness, the proposal for optional standard clauses is laudable but does not in itself provide any assurance.

A more effective cumulative solution could be to draw up a list of abusive or illegal clauses (such as in consumer law, see European Directive 93/13 / EEC of the Council of 5 April 1993, amended in 2011 by Directive 2011/83 / EU concerning unfair terms in consumer contracts, also known as the "CACC Directive"). Such clauses are also being considered, for example, as part of the proposed Digital Services Act and Digital Markets Act.

Finally, it is unclear from the latter question whether the solutions proposed would be horizontal or sectorial. Regarding the latter, we caution about using the PSD2 model horizontally. We stress yet again that any legislation should be based on a strict impact assessment, which does not at present in our view warrant a horizontal instrument.

Regarding data access at fair, reasonable, proportionate, transparent and non-discriminatory conditions, which of the following elements do you consider most relevant to increase data sharing? (The party sharing data obtains a reasonable yield on investment and the party requesting access to data pays a reasonable fee; distinctions can be made depending on the type of data or the purpose of its use; availability of standards for interoperability that would allow data sharing and exploitation at a low marginal cost (in terms of time and money); structures enabling the use of data for computation without actually disclosing the data; availability of an impartial dispute settlement mechanism; none of the above)

A generalised use of FRAND in legislation fundamentally misunderstands the link of this concept with the fields in which it is presently used (notably its special use in standardisation), which

cannot be generalised. Having said that, depending on the data access case under consideration one or more of the above listed options could be relevant.

SECTION III. Tools for data sharing: smart contracts

Are you using smart contracts or have you been involved in proofs of concept or pilots for Distributed Ledger Technologies that make use of smart contracts?

EACB members are at different levels of development/deployment in the use of smart contracts. Members are conducting work at experimental/project levels and production-ready applications. For example, some members are conducting projects to see where they can use smart contracts, the main area seems to be in capital markets. Although they highlight the costs of implementing a comprehensive infrastructure for smart contracts might not be worth the benefits. Others are looking into smart contracts from a custody and issuance perspective in the field of markets and investment banking, with the ambition to learn and start using this technology for issuing tokenized securities. In particular, they are looking at a proof of concept in the functionality of Ethereum blockchain using smart contracts based on Solidity. Others, for example, are looking at DLT-based trade finance applications meant to digitize the related workflows between trade participants.

On DLT in general, EACB members are unsure whether it is better than the existing processes; research in this area is still needed.

Do you consider that (when individuals request data portability from businesses) smart contracts could be an effective tool to technically implement the data access and use in the context of co-generated IoT data, in particular where the transfer is not only one-off but would involve some form of continuous data sharing?

EACB members believe that smart contract could be an effective tool but is only one component in data access and use. While smart contracts could be an element in implementing portability, they are not the only mechanism to this end. Standardisation of data pools and access thereto would arguably be more important and also needed.

EACB members are experimenting the use for smart contracts to see in what use cases they can represent a beneficial tool.

As to whether interoperability is an issue for scaling smart contracts, and what standardisation requirements (e.g., cybersecurity) could solve this issue, EACB members believe that interoperability is a cross-cutting issue and is not specific to smart contracts. Any technical solutions, which obviously also need to ensure proper cybersecurity (for example, by means of SOC2 compliance), must be left to standardisation organisations. Legal enforceability will also be key, especially in a cross-border environment.

SECTION IV. Clarifying rights on non-personal Internet-of-Things data stemming from professional use

EACB members find the questions in this Section in some cases too vague. EACB members are of the opinion that the IoT area in the banking sector is not mature enough, and that if specific issues are identified in specific sectors they should be dealt with under more targeted and appropriate sectorial instruments.

SECTION V. Improving portability for business users of cloud services

Was your organisation aware of the SWIPO Codes of Conduct prior to filling in this questionnaire? In your opinion, do the self-regulatory SWIPO codes of conduct on data portability developed by the cloud stakeholders represent a suitable approach to address cloud service portability?

Many of our members are aware of the SWIPO Codes of Conduct but they didn't participate in the drafting process. For the SWIPO process to be suitable, more balanced representation between cloud providers and users would be needed.

EACB members believe that the European Commission's project of a 'cloud rulebook' to offer a compendium of existing cloud codes of conduct is a good option to raise awareness and compliance of cloud service providers.

Do you consider there is a need to establish a right to portability for business users of cloud computing services in EU legislation?

EACB members believe that there is a need to establish a right to portability. From a legal point of view, a right to portability should be translated into a commitment to portability by cloud service providers towards users.

The scope of this right and obligation should cover data and applications as a minimum and the main elements such as deadlines, technical formats, recovery of transformed data.

What legislative approach would be the most suitable in your opinion, if the data portability right for cloud users would be laid down in an EU legislation?

A combination of high-level principles and more detailed contractual conditions would be needed to ensure a sufficiently detailed and actionable right for organizations. The specific technical conditions should not be detailed in legislation but be left to standards organisations.

Would it be necessary in your opinion to develop Standard Contractual Clauses for cloud service portability to improve negotiating position of the cloud users?

The right to portability for users and the commitment to portability for cloud providers can only be applied if this right/obligation results from a binding regulatory text. Supplementing this regulatory text with standard clauses that would address the issues of deadlines, formats, and the nature of the data returned or ported would be welcome to limit negotiation difficulties encountered with certain cloud service providers on these subjects.

SECTION VI. Complementing the portability right under Article 20 GDPR

We note that some questions of this Section are very much focused on user consent as a basis for data access. However, there are a series of legal bases already applicable both under the GDPR and the ePrivacy Directive, all of which are equally valid. User consent should therefore not be stressed as the only tool to enable data sharing.

SECTION VII. Intellectual Property Rights – Protection of Databases

Intellectual Property Rights

Intellectual Property is the basis of different business models and the company that owns it should have the right to determine who has access to this information and what will happen with it. Databases do not only contain personal data but also confidential information which may be protected by copyright or sui generis rights. It is important to enter into specific licence agreements in order to set forth the terms and conditions of use of such data and confidential information in order to avoid misappropriation of valuable data from third parties.

Database Directive

EACB members believe that public databases should be easily accessible in order to promote information sharing and, ultimately, innovation. In this sense, limiting the effect of the sui generis right of public authorities could be necessary, especially since there would be no impact on the economic survival of these entities contrary to the equivalent considerations for the private sector. It is without saying that when it comes to information security access rights, the same rules should apply for all market players.

There are crucial differences between public data/data generated by public authorities versus data generated by economic acting companies. For the former, there is a clear rational to "share" data (e.g., for health care or public traffic management), while the latter should be treaded based on bi-/multilateral contracts, freedom of contract and market economy.

Trade secrets protection

EACB members rely on the legal protection of trade secrets when sharing data with other businesses by contractual arrangements, e.g., a non-disclosure agreement, and by means of special cybersecurity solutions that also ensures confidentiality, such as encryption. They ensure control over the use of their data by other businesses, i.e., that it is not misused, misappropriated or disclosed unlawfully, by relying on the legal protection of trade secrets, on intellectual property rights and on contractual arrangements.

VIII. Safeguards for non-personal data in international contexts

What would be the best solution at an EU regulatory level to mitigate the risk for European companies stemming from the request for access by foreign jurisdiction authorities to their data?

It is important to note that the major cloud providers are creating partnership with EU companies to provide services compliant with EU regulation.

The suggested measures seem all appropriate (i.e., 1) introducing an obligation for data processing service providers to notify the business user every time they receive a request for access to their data from foreign jurisdiction authorities, to the extent possible under the foreign law in question; 2) introducing an obligation for data processing service providers to notify to the Commission, for publication on a dedicated EU Transparency Portal, all extraterritorial foreign

laws to which they are subject and which enable access to the data they store or process on behalf of their business users; 3) introducing an obligation for data processing service providers to put in place specified legal, technical and organisational measures to prevent the transfer to or access of foreign authorities to the data they store or process on behalf of their business users, where such transfer or access would be in conflict with EU or national laws or applicable international agreements on exchange of data; and 4) providing for compatible rules at international level for such requests).

It should be considered that most are already required under the applicable rules for transfers of personal data, which will be valid for the vast majority of data requests from third countries.

The fourth suggestion about compatible rules appears to be the most appropriate because it would tackle conditions and rules related to public bodies, which private actors cannot themselves tackle beyond possible legal, technical and organisational measures.

European companies need aligned political action to operate their businesses in a secure environment compliant with EU law.

Contact:

The EACB trusts that its comments will be taken into account.

For further information or questions on this paper, please contact:

- Ms Marieke van Berkel, Head of Department Retail Banking, Payments, Financial Markets (marieke.vanberkel@eacb.coop)
- Ms Chiara Dell'Oro, Senior Adviser for Digital Policies (chiara.delloro@eacb.coop)